

Admin Guide

ArcWeb Admin Guide

Lieberman Software Corporation

CONTENTS

LICENSE AGREEMENT	7
LIMITED WARRANTY	8
PRE-USAGE CONSIDERATIONS	11
INITIAL CONFIGURATIONS	13
The First Login Screen	14
Input The License	16
Configuration.....	18
Data Sources	19
Log Config.....	21
Verification	23
Adding or Updating Verification Questions.....	25
Domains	29
Domain Details	29
Security.....	30
Super Users	31
Management.....	33
Program Access.....	33
Group Access.....	34
Help Desk Reset Features	35
Self Reset Features.....	38
Configure Email Settings	42
Appearance	44
HOW TO USE ACCOUNT RESET CONSOLE.....	47
Accounts.....	48
Lookup/Reset	48
Change My Password	50
Change a Forgotten Password - Web.....	51
Change a Forgotten Password - Logon Provider	54
Setup My Identity.....	58
Scheduling/Reporting.....	61
View Logs	61
Account Tasks.....	62
View Task Results.....	67
Manage Synchronization.....	68
View Sync Results.....	70
INDEX	73

Copyright © 2003-2012 Lieberman Software Corporation.
All rights reserved.

The software contains proprietary information of Lieberman Software Corporation; it is provided under a license agreement containing restrictions on use and disclosure and is also protected by copyright law. Reverse engineering of the software is prohibited.

Due to continued product development this information may change without notice. The information and intellectual property contained herein is confidential between Lieberman Software and the client and remains the exclusive property of Lieberman Software. If there are any problems in the documentation, please report them to Lieberman Software in writing. Lieberman Software does not warrant that this document is error-free.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise without the prior written permission of Lieberman Software.

Microsoft, Windows, Word, Office, SQL Server, SQL Express, Access, MSDE, and MS-DOS are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Other brands and product names are trademarks of their respective owners.



Lieberman Software Corporation

1900 Avenue of the Stars

Suite 425

Los Angeles

CA 90067

310.550.8575

Internet E-Mail: ***support@liebsoft.com***

Website: ***http://www.liebsoft.com***

LICENSE AGREEMENT

This is a legal and binding contract between you, the end user, and Lieberman Software Corporation. By using this software, you agree to be bound by the terms of this agreement. If you do not agree to the terms of this agreement, you should return the software and documentation as well as all accompanying items promptly for a refund.

1. Your Rights: Lieberman Software hereby grants you the right to use User Manager Pro to manage the licensed number of systems purchased. This software is licensed for use by a single client and its designated employees, contractors and authorized 3rd parties to manage the systems owned/used by a single client. The software license may not be shared with unrelated 3rd parties.

The serial number provided by Lieberman Software is designed for installation on a specific machine. You may install an unlimited number of copies of User Manager Pro for your administrators that connect to the single licensed machine. All administrators can share the pool of purchased managed node licenses.

There are no limits to the number of web servers or clients that may access the data stored by your licensed copy of User Manager Pro. You may install and use the "User Manager Pro: Web Interface to Random Password Generator Password Recovery Console" with your duly licensed copy of User Manager Pro + Random Password Generator without any additional payment to Lieberman Software.

The cost of Microsoft web servers, SSL certificates, and other supporting equipment and technology are the sole responsibility of the user of this software-not Lieberman Software.

2. Copyright. The SOFTWARE is owned by Lieberman Software and is protected by United States copyright law and international treaty provisions. Therefore, you must treat the software like any other copyrighted material (e.g. a book or musical recording) except that you may either (a) make one copy of the SOFTWARE solely for backup and archival purposes, or (b) transfer the SOFTWARE to a single hard disk provided you keep the original solely for backup and archival purposes. The manual is a copyrighted work also--you may not make copies of the manual for any purpose other than the use of the software.

3. Other Restrictions: You may not rent, lease, or transfer the SOFTWARE to any other entity. You may not reverse engineer, de-compile, or disassemble the SOFTWARE that is provided solely as executable programs (EXE files). If the SOFTWARE is an update, any transfer must include the update and all prior versions.

4. Notice: This software contains functionality designed to periodically notify Lieberman Software of demo usage and of the detection of suspected pirated license keys. By using this software, you consent to allow the software to send information to Lieberman Software under these circumstances, and you agree to not hold Lieberman Software responsible for the use of any or all of the information by Lieberman Software or any third party.

When used lawfully, this software periodically transmits to us the serial number and network identification information of the machine running the software. No personally identifiable information or usage details are transmitted to us in this case. The program does not contain any spyware or remote control functionality that may be activated remotely by us or any other 3rd party.



Lieberman Software Corporation
1900 Avenue of the Stars
Suite 425
Los Angeles
CA 90067
310.550.8575

LIMITED WARRANTY

Internet E-Mail: ***support@liebsoft.com***

Website: ***http://www.liebsoft.com***

The media (optional) and manual that make up this software are warranted by Lieberman Software Corporation to be free of defects in materials and workmanship for a period of 30-days from the date of your purchase. If you notify us within the warranty period of such defects in material and workmanship, we will replace the defective manual or media.

The sole remedy for breach of this warranty is limited to replacement of defective materials and/or refund of purchase price and does not include any other kinds of damages.

Apart from the foregoing limited warranty, the software programs are provided "AS-IS", without warranty of any kind, either expressed or implied. The entire risk as to the performance of the programs is with the purchaser. Lieberman Software does not warrant that the operation will be uninterrupted or error-free. Lieberman Software assumes no responsibility or liability of any kind for errors in the programs or documentation of/for consequences of any such errors.

This agreement is governed by the laws of the State of California.

Should you have any questions concerning this Agreement, or if you wish to contact Lieberman Software, please write:

Lieberman Software Corporation
1900 Avenue of the Stars
Suite 425
Los Angeles
CA 90067

You can also keep up to date on the latest upgrades via our website at [**http://www.liebsoft.com**](http://www.liebsoft.com) or e-mail us at: [**sales@liebsoft.com**](mailto:sales@liebsoft.com).

PRE-USAGE CONSIDERATIONS

Please ensure completion of all steps as outlined in the Account Reset Console Installation Guide. The steps outlined in that guide outline SQL configuration, IIS configuration and recommendations, as well as COM account configuration requirements.

If there are any questions or concerns about this program's installation or operation before or after it has been installed, please contact Lieberman's support department for assistance. Incorrect installation or poor security practices could allow the compromise of passwords.

When used and installed properly, this program provides excellent performance, speed and security for password management. Call Lieberman Software if there are any questions about this product.

INITIAL CONFIGURATIONS

Following the initial installation of Account Reset Console, virtually nothing will be configured and no user be able to use ARC to reset other user's passwords or their own. The following sections describe the processes required to enable password management functionality, options available with Account Reset Console, what it means to turn on a specific option, and recommended practices.

The following sections are organized by navigation bar headings, those are the links found horizontally across the top of any page, and sub-organized by the navigation options found vertically under the left side of each navigation bar heading.

The screenshot shows the Account Reset Console interface. At the top, the Lieberman Software logo is on the right, and the text "Account Reset Console" is in the center. On the left, it says "Logged in user" with a red arrow pointing to "Log on user: LT\lanicu". Below the header is a "Navigation Bar" with four tabs: "Accounts", "Scaling/Reporting", "Management", and "Configuration". A red arrow points to the "Scaling/Reporting" tab. Below the navigation bar is a red bar labeled "Lookup / Reset". A red arrow points to this bar, and below it is a "Location Bar" with the text "Enter a user name to look up". The "Location Bar" contains a "User Name" input field, a "Domain" dropdown menu (currently showing "LT"), and a "Look up Answers" button.

IN THIS CHAPTER

The First Login Screen	14
Input The License	16
Configuration.....	18
Management	33

THE FIRST LOGIN SCREEN

Following the initial installation of Account Reset Console, nothing will be configured. This means that only users who are direct members of the 'super users' group configured during installation will be able to perform an initial login and configuration. Being a direct member means that the user account is found in the member of tab of the specified group as opposed to belonging to a group that belongs to that group.

To perform the initial login, type the user name, password, and choose the domain from the drop down list, then click the **Log In** button.



The screenshot shows the 'Account Reset Console' login interface. At the top, there is a red logo and the text 'LIEBERMAN SOFTWARE'. Below this, the title 'Account Reset Console' is displayed in large white letters. The main section is titled 'Please log in' and contains three input fields: 'User Name', 'Password', and 'Domain'. The 'Domain' field is a dropdown menu currently showing 'DEMO'. Below these fields is a 'Log In' button. At the bottom, there is a link 'Forgot your password / Locked out?' and a corresponding 'Reset Password / Unlock' button.

LIEBERMAN SOFTWARE

Account Reset Console

Please log in

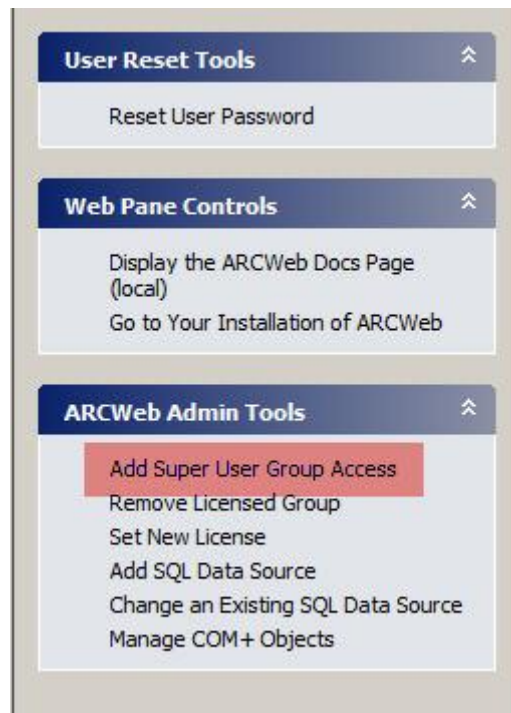
User Name

Password

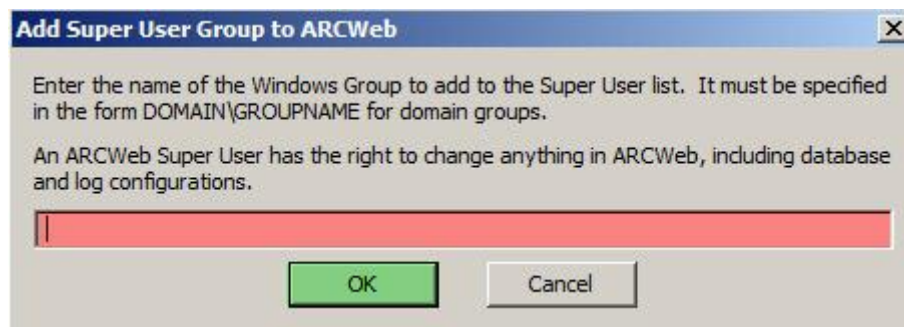
Domain

[Forgot your password / Locked out?](#)

If the login account is not a member of the super users group, during the first login following the tool's configuration, the login account will be unable to log in. To fix this, use the ARC Admin Console (ArcAdminConsole), found in the ArcWeb folder on the host systems start menu. Click the **Add Super Users Group** link and type the name of a group in which the login account is a direct member. Once logged into the website further changes may be made to the delegation structure.



Type in the group name as DomainName\GroupName such as 'domain\domain admins'. Click **OK** to continue. A confirmation that the group was added successfully will appear.



INPUT THE LICENSE

If this is a fresh installation of Account Reset Console, then following the successful installation of Account Reset Console, the license will also need to be configured. If this is an evaluation of Account Reset Console, licensing may be skipped as ARC ships with a fully functional 30 day license for 100 users.

Licensing may be configured using the ARC Admin Console or the ARC web site. To configure licensing using the ARC Admin Console, skip to the next step.

To configure a license for ARC using the website, log into ARC as a member of the super users group and go to **Configuration | Licensing**.

Input the license and click the Update License Key.

Logged in user:LT\lanicu [Logout]

Accounts Scheduling/Reporting Management Configuration

Licensing

Current License Details

Computer Name	
Serial Number	
	Update
Managed User Count	843
	Recalculate
Managed User Timestamp	3/19/2012 12:01:21 PM
Version	5.5 (120314)
Maximum Users	5000
License Expiration Date	[never]
Support Expiration Date	10/30/2012 11:53:53 AM

If the key is accepted, the page will refresh and the text ******* License Key Updated ******* will appear in the above page.

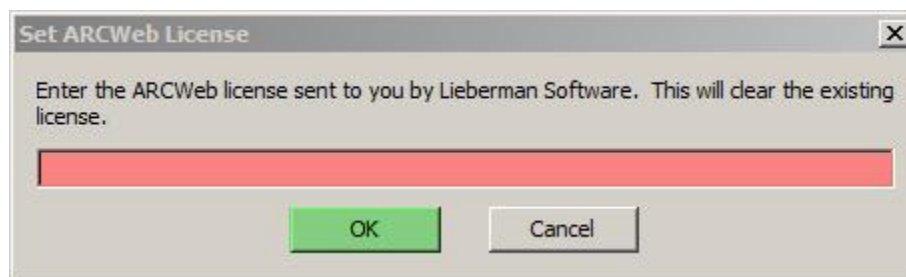
Following the initial installation, if licensing was configured using the website, the following steps need not be performed.

To configure a new license using the ARC Admin Console, launch **ArcAdminConsole** from the **ArcWeb** folder found under the host system's Start menu.

Click on the **Set New License** link in the **ArcWeb Admin Tools** section.



Enter in the new/updated license key and click **OK**.



If the key is accepted, the following dialog will appear. Click **OK** to continue.



CONFIGURATION

In Account Reset Console, there are many settings. The settings pertaining to global program operation are controlled through the **Configuration** area.

The **Configuration** area is used to configure the following items:

- ▶ **DATA SOURCES** - data sources are used for logging databases for the actions that occur within ARC and are used for storage and retrieval of user verification questions. Configure the server and database that ARC will connect to and the method for how ARC will connect to it from this page; this area does not identify what the databases will be used for. The issue of how a given database will be used once configured for use is addressed in either the **Log Config** or **Verification** [Q&A for Self Service] areas.
- ▶ **LOG CONFIG** - Identify the database (previously configured under data sources) that you would like ARC to log its use information to.
- ▶ **VERIFICATION** - Define the questions that will be used for self service reset. Self service reset allows a user to reset their own password when they have forgotten it without involving your help desk. When defining a question, you may choose to use the **default database** or you may identify other data sources (previously configured under data sources) to store and / or retrieve questions and answers from.
- ▶ **DOMAINS** - identify the default domain that appears in the drop down list during logon, password reset operations, and delegation changes. Also identify what domains may be managed if multiple trusting domains exist. This area is also used to identify preferred domain controllers and validate connectivity to target domains.
- ▶ **SECURITY** - Configure session timeout and approved characters that can be used for self service reset operations.
- ▶ **SUPER-USERS** - Groups defined here have complete control of the application regardless of any other rights.
- ▶ **LICENSING** - Input a new license for ARC to use and see how many user accounts are being managed by ARC.

Following a fresh installation of Account Reset Console, there is nothing else which must be configured with the exception of delegation rules that allow groups of users to reset other groups of user's passwords. This is handled in the **Management** area.

It is recommended to configure a default domain. For steps to do this, go to the **Domains** option found under **Configuration**.

The following pages outline the Configuration options.

DATA SOURCES

To configure data sources for ARC to use for verification questions or logging, go to **Configuration | Data Sources**.

Data sources are databases that are defined within ARC and are used for:

- ▶ LOGGING DATABASES - Actions that occur within ARC such as logging in or resetting a user's password.
- ▶ VERIFICATION QUESTIONS - Data sources define the databases that will be used to store and retrieve answers to a user's verification questions.

When configuring a data source, configure the server and database that ARC will connect to and the method for how ARC will connect to it; this area does not identify what the databases will be used for. The issue of how a given database will be used once configured for use is addressed in either the **Log Config** or **Verification** areas. If a database will be used to store questions that will be used for verifying a user's identity to allow for self service password reset or account unlock, then use the **Verification** link from the action menu.

If this is the first time examining this page, notice there is already a data source that is configured with a name of **Default Database**. This is the database that was configured during the installation of Account Reset Console and is the default location for all logging and verification questions and answers. If any settings should change about that database such as server name, database name, or authentication method, select the **Edit** link inline with the named database.

To add a new data source to use for logging or verification questions, supply the following information:

- ▶ **NAME** - this is the friendly name as it will appear in drop down lists within this tool
- ▶ **TYPE** - the type of database we are connecting to. Any ODBC/OLEDB data source can be used to retrieve or write information to. Choices are Microsoft SQL, or Explicit ADO connection string which is used for connecting to non-Microsoft databases.

Once this information is identified, click the **Add** button.

Configure Existing Data Sources

Name	Type	Working	LogDB	Actions
Default Database	SQL Server	✓	✓	Edit Delete

Add New Data Source

Name

Type

Microsoft SQL Server

Add

When first adding a new data source, the **Working** column will be labeled with a red X. This indicates that the database is not configured. Select the **Edit** link in order to finish setting up the data source.

In order to properly configure an ADO data source, the complete connection string which includes the server, database, and account information required to connect will be required.

In order to properly configure a Microsoft SQL data source, the following information must be supplied:

- ▶ **SERVER INSTALLATION** - this is the name of the database server and any instance naming information. For example, a default instance of MS SQL, will simply be addressed by the server name. An instance of MS SQL using a named instance will be addressed as ServerName\InstanceName as noted in the screen shot below.
- ▶ **DATABASE NAME** - the is the name of the pre-existing database to use on the specified server
- ▶ **AUTHENTICATION TYPE** - choices are **Windows Authentication** or **SQL Server Authentication**. It is recommended to use Windows Authentication which will use the integrated authentication token of the COM object to authenticate to the database. This method does not require a password to be stored in the connection string used to connect to this database.

Once these settings are entered, click **Save Data Source Settings**. The connection will be verified at this time. If there are no problems, this page will refresh and the **Status** notification at the bottom of this page will display a green check mark next to your database with a status of **OK**.

Edit Data Source
Name: ARCDDB
Type: SQL Server
Server Name:
Database Name:

Authentication
☐ Windows Authentication
☒ SQL Server Authentication
User Name:
Password:
Status: Not Working

LOG CONFIG

To configure Logging database settings go to **Configuration | Logging**.

The Log Config is used to identify the database (previously configured under data sources) that ARC should use to log its use information to. By default, ARC will use the database (default Database) configured during program installation.

If additional data sources have been configured in the Data Sources area, it is possible to use change the logging database to one of these data sources. If the required tables used to log the information are missing form the data source, ARC will attempt to automatically create the missing table.

Note: If the logging database is changed, information previously logged will not be copied or duplicated in any way to the new database.

Once logging database has been changed by selecting it from the **Logging Data Source** drop down menu, click the **Update Logging Settings** button. Once the update is complete, the status will change to **OK**.

Current Settings

Name: Default Database
Type: SQL Server
Status:  OK

Update Settings

Logging Data Source: 

VERIFICATION

To configure verification questions go to **Configuration | Verification**.

The **Verification** area is used to define the questions that will be used for user verification during self service password reset or help desk initiated password reset of a user.

Self service password reset allows a user to reset their own password when they have forgotten it without involving the help desk. When defining a question, possible data storage/retrieval locations are the **Default Database** or other configured data sources.

Account Reset Console ships with three pre-existing questions that are configured as **inactive**. Before any user can take part in self service password reset via ID verification, there must be at least one active question. Questions may be added to the active pool by selecting the **Activate** link next to the question. Questions may be added, edited, or deleted entirely by using the respective **Add Questions**, **Edit**, or **Delete** links.

If any changes are made to the status of the questions, be sure to save the new settings using the **Save Verification Options** button at the bottom of the page.

To add more verification questions, type in the text of the question in the **Question Text** field then click **Add Question**. This will add the question without any settings to the **Inactive Questions** list. Once the question is configured, it may be added to the **Active Questions** list by selecting the **Activate** link found inline with any inactive questions. For further information on adding or editing verification questions, see the next section, **Adding or Updating Verification Questions**.

Configure User Identity Verification Questions Here

Active Questions

Question Text	Action
What is your first pet's name?	Deactivate Delete Edit
What is your mother's maiden name?	Deactivate Delete Edit

Number of questions user has to answer

Inactive Questions

Question Text	Action
This is question 1	Activate Delete Edit
What is your favorite color?	Activate Delete Edit

Add New Questions

Question Text

Add

The second portion of the Verification page allows defining if a notification will occur when a user attempts to update their verification question(s) and who those notifications will go to. The user may be notified of a successful or failed update. In order to notify the user, ARC will retrieve their primary e-mail address from Active Directory. If not using Active Directory or this attribute is not configured; the user cannot be notified.

The e-mail can be configured as plain text or HTML. Choosing to format the e-mail as HTML will require you to use HTML to write the e-mail.

There are a list of variables which may be used within the e-mails at the bottom of this page.

When a User Updates Verification Answers

☐ Notify user of successful update

☐ Notify user of failed update

Dear #RealName#,

This is an automatic notification that your account verification questions used for self-service password reset have been recently modified or were attempted to be modified. If you did not recently attempt to update your verification answers, you should

☐ Plain Text ☒ HTML Mail

Help desk and the ARC admin may also be notified of successful or failed updates to the user's verification answers. The e-mail addresses used for the help desk and arc admin are defined with the **Configure Email Settings** action in the **Management** area.

The e-mail can be configured as plain text or HTML. Choosing to format the e-mail as HTML will require the use of HTML to write the e-mail.

There are a list of variables which may be used within the e-mails at the bottom of this page.

☐ Notify help desk of successful update

☐ Notify help desk of failed update

☐ Notify admin of successful update

☐ Notify admin of failed update

#UserName# (#RealName#) has just attempted to update their password verification questions and #Result#.

☐ Plain Text ☒ HTML Mail

Email Keywords:

#RealName#

- User's full name as stored in Active Directory.

#UserName#

- User's logon name.

#IPAddress#

- IP Address.

#Time#

- Current time.

#Result#

- User resets password result.

Save

If any changes are made to this page, be sure to save the new settings using the **Save Verification Options** button at the bottom of the page.

ADDING OR UPDATING VERIFICATION QUESTIONS

Account Reset Console ships with three pre-existing questions that are configured as **Active**. This means a user will be required to answer these questions in order to participate with self service reset. A question may be removed from the active pool by selecting the **Deactivate** link next to the question or deleted entirely. A question may be edited by selecting the **Edit** link. Editing a question will allow changing its text, and database query strings.

To add more verification questions, type in the text of the question in the **Question Text** field then click the **Add Question** button. This will add the question without any settings to the **Inactive Questions** list. Before the question will be asked of a user, the question must first be edited and assigned to a data source, and then choose to **Activate** the question.

Configure User Identity Verification Questions Here

Active Questions

Question Text	Action
What is your first pet's name?	Deactivate Delete Edit
What is your mother's maiden name?	Deactivate Delete Edit

Number of questions user has to answer

Inactive Questions

Question Text	Action
This is question 1	Activate Delete Edit
What is your favorite color?	Activate Delete Edit

Add New Questions

Question Text

Add

Before a question can be used, identify which database to use and who must answer the question.

Presented for all users means all users who enroll must provide an answer to the question. **Presented for the following selected groups** means only users who belong to the identified groups will be required to answer the question. Enter the group name as DomainName\GroupName.

Edit Verification Question

Question Text:

Target User

☒ Presented for all users
☐ Presented for the following selected groups

Add

Which database to use? The default database is the database that is configured during the installation of ARC. It is also the database that is used for logging by default. This is the best choice to use if the answers will not be pre-populated but rather supplied by users via an enrollment process.

Use a custom verification database to read and/or write user answers from a non-Microsoft SQL database or if retrieving answers from other data sources such as Lotus Notes, Active Directory, or some other HR database. For example, to retrieve the last four of a user's social security number from an HR database, use the custom database.

Data Storage

☒ Use current active database for verification
 ☐ Use custom verification database

Data Source

Default Database

Queries

Retrieval:

If your retrieval query is not working, please ensure that you have records in the appropriate database for your test user.

☒ Allow users to set their own answers to this question
 ☐ Answer is in plain text

Setting:

Insertion:

Examples

Retrieval: `select Answer from CustomerTable where UserName = '#USER#' and DomainName = '#DOMAIN#' and ID = '#GUID#'`
 Setting: `update CustomerTable set Answer = '#ANSWER#' where UserName = '#USER#' and DomainName = '#DOMAIN#' and ID = '#GUID#'`
 Insertion: `insert into CustomerTable ( UserName, DomainName, ID, Answer ) values ('#USER#', '#DOMAIN#', '#GUID#', '#ANSWER#')`

Save

Return

To use a custom database, the data source must have been previously defined in the Data Sources section of the Configuration area. Also provide retrieval, setting, and insertion queries. The following examples are the minimum queries for each of the three query strings.

- ▶ Retrieval - used to retrieve user answers:
`select QuestionAnswer from ARC_VerificationAnswers where UserName = '#USER#' and DomainName = '#DOMAIN#' and QuestionGUID = '#GUID#'`

If a user should not be able to update the answer in the target data source, clear the check box next to **Allow users to set their own answers to this question**.

- ▶ Setting - used to update user answers to custom database via ARC. Leave this blank if users will not be allowed to edit their own answers:
`update ARC_VerificationAnswers set QuestionAnswer = '#ANSWER#' where UserName = '#USER#'`

and DomainName = '#DOMAIN#' and QuestionGUID = '#GUID#'

- Insertion - used to add user answers to custom database via ARC. Leave this blank if users will not be allowed to add their answers:

```
insert into ARC_VerificationAnswers ( QuestionGUID, UserName, DomainName, QuestionAnswer )  
values ('#GUID#', '#USER#', '#DOMAIN#', '#ANSWER#' )
```

Once the questions are configured, click **Save Settings** at the bottom of the page. There is no visual indication that the question was saved. Then choose **Return to Question List**.

Inactive Questions			
Question Text	Action		
This is question 1	Activate	Delete	Edit
What is your favorite color?	Activate	Delete	Edit

Questions may then be activated for use. When a question is activated, it will be moved from the inactive questions list to the active questions list. Similarly, deactivate questions by clicking on the **Deactivate** link which will move the question to the inactive questions list from the active questions list.



DOMAINS

To configure authentication domains, go to **Configuration | Domains**.

The **Domains** section is used to define three things:

- ▶ Which domains to manage
- ▶ Which domain controller in each domain to prefer
- ▶ And what should be the default domain

When this page is displayed, it will only show domains that have been selected for management by selecting the check box in the **Manage** column. By default this is the local system and the local domain. If the status is a green check mark, then your COM account has at least the minimum rights to reset passwords. If there are additional trusting domains to manage and the COM account (configured during installation) has the required permissions to manage those domains, clicking the **Show All** link towards the top right corner and enabling the check box in the **Manage** column will permit ARC to manage user's passwords in those domains - delegations permitting.

To see more information about a given domain including the preferred domain controller for password changes, select the **Details** link. For more information on this, see the next section, **Domain Details**.

Managed Domains and Domain Controllers					
Default	Managed Domain	Primary Domain Controller	Manage	Status	Actions
☐	DEMO	2K8R2-DC	☒	✓	Details
☐	DEMO2	2K8R2-DC-DEMO2	☒	✓	Details
☒	[local]		☒	✓	
					Save

The **Default Domain** defines what domain will be automatically displayed in domain selection drop down lists. Following installation, this is defaulted to **[local]**.

If any changes have been made which should be saved, click **Save Domain Configuration**. There will be no further confirmation of changes to these options. To discard any changes you have made, simply navigate away from this page without clicking Save Domain Configuration.

DOMAIN DETAILS

When viewing the details of a domain, the COM account will attempt an administrative connection to the preferred domain controller to gather the status of this domain. If the COM account is not an

administrator on the domain controller, this will fail and status information will not be retrieved. This error can be ignored.

From this page a preferred domain controller from which to perform password changes may be selected. By default, ARC will attempt to use any available domain controller with a preference to the domain controller holding the PDC Emulator role. If that machine is unavailable, ARC will try another domain controller from the list of available domain controllers. To change this behavior to change and use a particular DC, simply click the link next to the preferred domain controller that says **Set as Default DC**.

Later, to revert to the default behavior, choose the link that says **Use any available DC** next to the Default Domain Controller.

Edit Domain Configuration

Domain Name	DEMO
Primary Domain Controller	2K8R2-DC
Domain Controller Status	2K8R2-DC:Success
Default Domain Controller	2K8R2-DC Use any available DC
Domain Controller List	2K8R2-DC 2K8R2-DC2 Set as Default DC
	Check All Domain Controller Status

Domain Details

Admin Privileges Check Code	0
Admin Privileges Check Description	
Domain is Managed	True
Last Error Code	0
Last Error Description	

SECURITY

Security is located in the Configuration area.

The Security section defines session timeout - how long before ARC kills an idle session. The security section also defines an allowed character set which are the characters that are allowed for verification answers (not case sensitive).

The default sessions timeout is 20 minutes. The default allowed character set is 'ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890 ' without the quotes. Note that there is a blank space following the 0. If the space is removed, users will not be allowed to use spaces in their verification questions. **Also note that no punctuation is allowed in the default character set. This is the preferred setting to avoid complications with various data sources that treat punctuation in different ways.**

It is recommended to not change the allowed character set.

The **Technical Support** field allows a message to be specified in the event of a password change error.

If changes are made to this page, click the **Save** button at the bottom of the page. There will be no further confirmation of changes to these options. If changes were made but the settings have not been and should be discarded, simply navigate away from this page without clicking Save button.

Session timeout:

The session timeout controls how many minutes a web browser session will remain logged-in without activity.

Allowed charset:

The allowed character set controls which characters (case-insensitive) will be accepted as valid characters for verification answers. For safety reasons, '()"[];,:\$=%*#?' are not recommended.

Technical Support:

Save

SUPER USERS

To configure Super Users, go to **Configuration | Super Users**.

Groups defined here in the **Super-Users** section have full control of the ARC application regardless of any other delegated rights or lack thereof including changing delegations, manipulating data sources, changing security, etc.

By default, this list contains only the group identified during installation of Account Reset Console. To add a new group to the list of super users, choose the correct domain and enter their group name in the group name field towards the top right of this screen, then click **Add Super Users**. If the add is successful, the group will appear in the list below as an **Allowed Windows Group**.

To remove a group, simply click the **Delete** link next to the group name.

Global Program Access Rules

Global Access Category	Allowed Windows Groups	
Allow application config	demo\domain admins	Delete

Add a New Application Superuser Group

DEMO	▼	Enter Group Name Here	Add
------	---	-----------------------	-----

MANAGEMENT

The settings defined in **Management** are for delegations (resetting of other user's passwords), self service reset abilities, appearance, and email settings. There are many settings which can be made here which change the user's experience when resetting another user's or their own password. Incorrect settings made here can block ARC from working. Please be sure to read about the settings when making changes.

PROGRAM ACCESS

To configure Program Access, go to **Management | Program Access**.

The Program Access section is the first part of delegating access to the console. This section provides global access to the ARCWeb console, but it does not grant the rights to reset other user's passwords. To control the rights of users who can reset other user's passwords, configure settings in the **Group Access** section as well.

ARC does not perform recursive queries to determine group membership. Intended users must be direct members of the delegated groups.

Rights are cumulative. If a user belongs to two or more groups granted access in this page, that user will be granted all of those rights.

The rights defined on this page are:

- ▶ ALLOW WEB LOGON - groups granted this right can log into the Account Reset Console. This right must be granted in order for any user to use this tool.
- ▶ VIEW CONSOLE LOGS AND TASK REPORTS - this in conjunction with the **Allow Web Logon** right will allow users assigned this right the ability to logon and view the activity that takes place in this web application. These logs are available in the **View Logs** section of the **Scheduling/Reporting** area.
- ▶ MANAGE ALL WEB ACCESS CONTROLS - grants users the rights to change all delegations and options available in the **Management** area. This does not grant any configuration rights for any options or settings in the **Configuration** area.
- ▶ REQUIRE WEB LOGON WITH RSA - will require the group of users to use RSA two-factor authentication. This is only visible when the RSA client (supplied by RSA) is installed and functioning on the ARC host system.

By default the group identified as the super-users group during setup listed for each right.

To add a group for user access, select the rights to assign from the top left of the page then add the group name in the top right corner and click the **Add** button. The group name will appear in the **Allowed Windows Groups** column.

Global Program Access Rules

Global Access Category	Allowed Windows Groups	
Allow Web Logon	demo\domain admins	Delete
View Console Logs and Task Reports	demo\domain admins	Delete
Manage All Web Access Controls	demo\domain admins	Delete

Add a New Global Program Access Rule

☐ Allow Web Logon

☐ View Console Logs and Task Reports

☐ Manage All Web Access Controls

☐ Require Web Logon with RSA

DEMO

Enter Group Name Here

Add

Once a group has been allowed access, those rights may be removed at a later date. To remove an assigned right from a group, click the **Delete** link to the right of the group name.

GROUP ACCESS

To configure Program Access, go to **Management | Group Access**.

To allow users to reset their own passwords, no configurations need to be made to this page. However, certain options in the **Self Reset Features** section must be enabled.

The **Group Access** section is used to delegate rights to reset passwords for specific groups of users. In order for a user to reset another user's passwords, the people resetting passwords must be in the **Administrative Group** and the people having their passwords reset must be in the **Managed Group**.

ARC does not perform recursive queries to determine group membership. Your intended users must be direct members of the delegated groups.

Rights are cumulative. If a user belongs to two or more groups granted access in this page, that user will be granted all of those rights.

To allow a group of users to reset passwords, enter their group name in the administrative group name field. Then identify which group of users they can reset by specifying that group name in the managed group name field. Finally, select the **Reset Password** right check box.

Additionally, you may elect to allow administrative groups to view a particular managed group's verification answers. This is useful when help desk will be performing password resets for users and you wish for those help desk users to validate the identity of those users using the verification questions.

Group Access Rules - Account Reset Privileges		
Administrative Group	Managed Group	
DEMO\can reset passwords	DEMO\self service reset	Delete

Group Access Rules - View User Answers Privileges		
Administrative Group	Managed Group	
DEMO\can reset passwords	DEMO\self service reset	Delete

Add a New Group Access Rule			
Administrative Group:	DEMO	can reset passwords	
Managed Group:	DEMO	self service reset	
Permissions:	☒ Reset Password	☒ View User Answers	Add

HELP DESK RESET FEATURES

To configure Help Desk Reset Features, go to **Management | Help Desk Reset**.

Help Desk Reset Features are the settings that apply to users resetting other users passwords using Account Reset Console. For settings that apply to users resetting their own passwords, see the section for **Self Reset Features**.

The first setting, **Reset passwords through Account Reset Console** is the global setting to enable the functionality allowing users to reset other user's passwords. To allow users to reset other user's passwords, this setting must be enabled.

The **Minimum number of questions help desk has to ask** is only valid if user's have enrolled with the verification questions. If a user [who is having their password reset] has enrolled with verification questions and this setting is set to a number higher than 0, the help desk must ask the user that many verification questions. If the user has not answered that many questions, or there are not that many questions configured, then the help desk user will need to ask the user every question they have enrolled with.

The next three options deal with specific user account flags and the preferred behavior of ARC in dealing with those flags when a user account is reset.

- ▶ **ENABLE DISABLED ACCOUNTS** - if an account has been disabled by an administrator, ARC can re-enable the account by resetting its password. It is recommended to set this to optional or never.
- ▶ **UNLOCK LOCKED ACCOUNTS** - if an account has become locked out because of failed login attempts, ARC can unlock the account by resetting its password. It is recommended to set this to optional or always.
- ▶ **REQUIRE THAT RESET PASSWORDS BE CHANGED ON NEXT LOGIN** - this will set the password must be changed at next login flag on the users account which will force the user to change the password on next login. For web applications or other interfaces that are incapable of resetting a user's password this may pose a problem as the user will be unable to change their password the next time they login and may be unable to access resources until they have access to a Windows system. The downside of not setting this flag is that now the help desk user and the user both know the password. It is recommended to set this to optional or always.

By default these items are set to optional which means that a help desk user will have the choice to perform or not perform these actions, by default the action will be performed. When the options are set to never, the tool will not show these options during a password reset and the tool will not perform these actions. When the options are set to always, the tool will not show these options and the tool will always perform these actions.

Prevent help desk from seeing the answer is designed to mask the verification answers of users when a help desk user is typing in the verification answer during reset of another user's password. If this option is not set, ARC will display the typed text in clear text, making it visible to the help desk user and anyone else who may be shoulder surfing or taking screen shots.

Help Desk Reset Features

☒ Reset passwords through Account Reset Console

Minimum number of questions help desk has to ask:

(Note: A value of 0 will allow the help desk to reset the user's password without verification.)

Enable account if disabled:

☐ Always

☒ Optional

☐ Never

Unlock locked accounts:

☐ Always

☒ Optional

☐ Never

Require that reset passwords be changed on next login (ignored when user cannot change password):

☐ Always

☒ Optional

☐ Never

☒ Prevent help desk from seeing the answer

Display the following HTML message... creates a heading at the top of the Account's page that is visible to users resetting other user's passwords.

☐ Display the following HTML message to help desk personnel resetting accounts

When a help desk user attempts to reset a user's password setting will notify the user that their password has been reset by a help desk user. In order to notify the user, ARC will retrieve their primary e-mail address from Active Directory. If Active Directory is not being used or this attribute is not configured, the user cannot be notified.

The e-mail can be formatted as plain text or HTML. Choosing to format the e-mail as HTML will require you to use HTML to write the e-mail.

There is a list of variables which may be used within the e-mails at the bottom of this page.

When a Help Desk User Resets a User Password

☐ Notify user of successful update

☐ Notify user of failed update

Dear #RealName#,

This is an automatic notification that your help desk's action to reset your user account's password has resulted in #Result#.

☐ Plain Text ☒ HTML Mail

The help desk may be notified of successful or failed updates to the user's password. The e-mail addresses used for the help desk and arc admin are defined in the **Configure Email Settings** area in the **Management** section.

The e-mail can be formatted as plain text or HTML. Choosing to format the e-mail as HTML will require you to use HTML to write the e-mail.

There is a list of variables which may be used within the e-mails at the bottom of this page.

☐ Notify help desk of successful update

☐ Notify help desk of failed update

The action by #HDUser# to reset the password for #UserName# (#RealName#) has resulted in #Result#.

☐ Plain Text ☒ HTML Mail

The ARC admin may be notified of successful or failed updates to the user's password. The e-mail addresses used for the help desk and arc admin are defined in the **Configure Email Settings** area in the **Management** section.

The e-mail can be formatted as plain text or HTML. Choosing to format the e-mail as HTML will require you to use HTML to write the e-mail.

There is a list of variables which may be used within the e-mails at the bottom of this page.

☐ Notify admin of successful update
☐ Notify admin of failed update

The action by #HDUser# to reset the password for #UserName# (#RealName#) has resulted in #Result# at #Time# from #IPAddress#.

☐ Plain Text
 ☒ HTML Mail

Email Keywords:

#RealName#	-	User's full name as stored in Active Directory.
#UserName#	-	User's logon name.
#Email#	-	User's email address as stored in Active Directory.
#Password#	-	The user's new password.
#IPAddress#	-	IP Address.
#Time#	-	Current time.
#RealName#	-	User's full name as stored in Active Directory.
#HDUser#	-	Help Desk User Name.
#Result#	-	Help Desk resets password result.

Save

Once changes are made to this page, click the **Save Program Features** button at the bottom of the page.

SELF RESET FEATURES

To configure Self Reset Features, go to **Management | Self Reset**.

The **Self Reset Features** section is for configuring all of the options surrounding a user resetting their own password or unlocking their own account, whether through the web interface, question verification, or through the credential providers, without help desk intervention. To guarantee that only help desk users could use this tool to change other user's passwords, every option on this page should be de-selected.

To allow users to reset their own password, *when their current password is not forgotten*, enable **Allow users to change their own passwords by logging into ARC**. When users change their own passwords, ARC will default to using the authority and credentials of the COM object (see installation guide) that runs ARC. This has the same effect of performing an administrative password reset. This means that users have the potential to bypass domain password policies such as password history and minimum age. To ensure users adhere to defined domain policies, enable the option to **Emulate the user account**

to comply with domain policies. When users change their own passwords, ARC also provides the option expire them so that they must be changed on next login - generally this option should not be enabled. ARC can also display a useful message to users resetting their own password in this scenario. The message can be input in standard text or by using HTML formatting. To create a custom message to display to users when they are resetting their own password, enable **Display the following HTML message to users resetting their own passwords.**



Change My Password Features

- ☒ Allow users to change their own passwords by logging into ARC
- ☒ Emulate the user account to comply with domain policies
- ☐ Display the following HTML message to users resetting their own passwords

Use the **Forgotten Password & Locked Out Features** to allow users to reset their password or unlock their own account when the users current password is unknown or their account is locked out. Usage of these features does not require the involvement of help desk. Enabling these features is not a requirement for users to reset their own password via ARC when the current password is NOT forgotten. To allow a user to reset their current password when the current password is not forgotten, use the **Change My Password Features** in the **Accounts** area.

Account Reset Console provides two alternatives for users to reset their own password or unlock their own account when the current password is unknown. These available options are to perform these operations from the ARC website or from a Logon Provider. The Logon provider is an additional component that would typically be installed on end-user's workstations. Proper installation of the Logon Provider will create an additional element on the CTRL-ALT-DEL dialog of a Windows system. With this option, a user will not need to have access to a kiosk or a neighbors computer. The options pertaining to website usage are labeled as **(Website)**. The options pertaining to the Logon Provider are labeled as **(Logon Provider)**. In either scenario, a user will have pre-enrolled with a series of [admin defined] verification questions. These questions will be asked of the user when they begin the process whether they are performing this from the website or from the Logon Provider.

To allow a user to reset their own account via ID verification, enable the **Allow users to reset their own password via ID verification** option. To allow a user to unlock their own account via ID verification, enable the **Allow users to unlock their own account via ID verification** option.

When a user is answering questions, it is possible that the user may have forgotten which answer they actually provided to a question. **Allowed incorrect answers before account lockout** is the number of times a user may answer a verification question incorrectly before ARC will lock the user out of the *self reset process* for the number of minutes defined in the **Account lockout timeout (minutes)**. When there

are multiple verifications defined and answered, ARC can randomly choose some or all of those questions to ask the user during the ID verification process. To have ARC randomly select verifications enable **Randomly choose verification questions from user's pool of questions** and then define the number of random questions to ask by putting a valid number in the **Number of verification questions users must answer** field. If a user fails the ID verification, ARC can notify the administrator and help-desk (email addresses defined in the email setting section) by enabling **Send verification failure to Administrator and Help Desk**.

Forgotten Password & Locked Out Features

- ☒ Allow users to reset their own passwords via ID verification (Website)
- ☒ Allow users to unlock their own account via ID verification (Website)
- ☒ Allow users to reset their own passwords via ID verification (Logon Provider)
- ☒ Allow users to unlock their own account via ID verification (Logon Provider)
- Allowed incorrect answers before account logout:
- Account logout timeout (minutes):
- ☒ Randomly choose verification questions from user's pool of questions
- Number of verification questions user must answer:
- ☐ Force user to change password on next login
- ☒ Send verification failure to Administrator and Help Desk

The **Verification Answers Features** subsection places constraints on the user's answers that may be provided for the verification questions during the ID verification enrollment process. To help users properly fill out their verification answers the first time, enable **Display identity answer requirement**. This option will display the elements to the user for a proper verification during the enrollment process. To stop the user from entering repeated strings of characters, enable **Do not allow repeated character patters such as 'AAAA'**. Users will often input the text of the question as their answer. To stop this behavior, enable **Do not allow the answer to contain text from the question**. However, if the user still includes additional text, they may work around this rule. To stop users from re-using the same answer to all questions, enable **Do not allow questions to contain duplicate answers from other questions**. As an example, the user would not be able to put in the answer 'red' more than once. To stop the user from supplying a blank answer to the question, enable **Require a minimum character length for each answer** and identifies how many characters a user must input for their question's answers.

Verification Answers Features

- ☐ Display identity answer requirement
- ☒ Do not allow repeated character patterns such as 'AAAA'
- ☒ Do not allow the answer to contain word from the question
- ☒ Do not allow questions to contain duplicate answers from other questions
- ☒ Require a minimum character length for each answer:

When a user attempts to reset their own password, ARC can notify the user that this process was even attempted. This is designed to keep the user aware of the goings on of their own account. In order to notify the user, ARC will retrieve their primary e-mail address from Active Directory. If not using Active Directory or this attribute is not configured, the user cannot be notified by ARC. The e-mail as plain text or HTML. Choosing to format the e-mail as HTML will require using HTML to write the e-mail. There are a list of variables which may be used within the e-mails at the bottom of this page.

When a User Resets Own Password

- ☐ Notify user of successful update status
- ☐ Notify user of failed update status

☐ Plain Text ☒ HTML Mail

Help desk may be notified of successful or failed updates to the user's password. The e-mail addresses used for the help desk and arc admin are defined in the **Configure Email Settings** area in the **Management** section. The e-mail as plain text or HTML. Choosing to format the e-mail as HTML will require using HTML to write the e-mail. There are a list of variables which may be used within the e-mails at the bottom of this page.

☐ Notify help desk of successful update status

☐ Notify help desk of failed update status

The action by #UserName# (#RealName#) to update their user account with #Action# has resulted in #Result#.

Action Performed: #Action#

☐ Plain Text ☒ HTML Mail

The ARC admin may be notified of successful or failed updates to the user's password. The e-mail addresses used for the help desk and arc admin are defined in the **Configure Email Settings** area in the **Management** section. The e-mail as plain text or HTML. Choosing to format the e-mail as HTML will require using HTML to write the e-mail. There are a list of variables which may be used within the e-mails at the bottom of this page.

☐ Notify admin of successful update status

☐ Notify admin of failed update status

The action by #UserName# (#RealName#) to update their user account with #Action# has resulted in #Result# at #Time# from #IPAddress#.

Action Performed: #Action#

☐ Plain Text ☒ HTML Mail

Email Keywords:

- #RealName# - User's full name as stored in Active Directory.
- #UserName# - User's logon name.
- #Email# - User's email address as stored in Active Directory.
- #Password# - The user's new password.
- #IPAddress# - IP Address.
- #Action# - Unlock / Reset.
- #Time# - Current time.
- #Result# - The user's password self reset result.

Save

Once changes have been made to this page, click the **Save Program Features** button at the bottom of the page.

CONFIGURE EMAIL SETTINGS

To configure Email settings, go to **Management | Email**.

The email server settings are only required to use any of the notification options for user password reset/updates or for e-mailing scheduled report results.

SMTP Express is a standalone mail relay that can be installed on the local system and is used when ARC will not be allowed to connect directly to a mail server.

The preferred option is **Use External Server**, which allows connection to an SMTP mail server. At a minimum provide the server name. Many mail systems require user authentication. If this is true for the preferred mail server, then supply the user name and password.

Change the SMTP port number if it is appropriate for the preferred server. By default and typically, SMTP operates over port 25.



The form is titled "Email Server" and contains two radio buttons: "Use Local SMTP Express Server" (unselected) and "Use External Server" (selected). Below the radio buttons, there is a "Server Name" text field. To the right of the "Server Name" field is a checkbox labeled "This email server requires authentication". Below the checkbox are three text fields: "User Name", "Password", and "Port Number". The "Port Number" field has the value "25" entered.

The e-mail addresses defined on this page are the email addresses that are used for the various notification that may occur when a user resets or has their password reset.

Source - what email address the email appears to come from. If the mail server does not perform reverse lookup, it is generally acceptable to use any source address desired. If the server does perform reverse lookup, a legitimate email address may be required. Generally, it is always wise to use an e-mail address that appears to come from your company's domain.

Reply - if someone does hit the reply button, on the notification email, this is the address it will go to. If not monitoring user replies to these e-mails, supply a junk address such as 'donotrespond@nevergonnacheckit.never'.

Administrator - this is typically the administrator of ARC and is the email address referred to in ARC when reference is made to 'Administrator'. If multiple people should receive a notification, put in the address of a distribution group.

Help Desk - this is typically the help desk users of ARC or your company's help desk. This is the email address referred to in ARC when reference is made to 'Help Desk'. If multiple people should receive a notification, put in the address of a distribution group.

Email Address

Source	
Reply	
Administrator	
Help Desk	

Save

Once configuration changes have been made, click the 'Save Email Configuration' button at the bottom of the page.

APPEARANCE

To configure Appearance settings, go to **Management | Email**.

The appearance page is used to 'skin' or manipulate the look of Account Reset Console. Various visual elements such as banners, headers, footers, and colors for each of the elements within Account Reset Console can be controlled on this page.

- ▶ COMPANY TAG LINE - typical use is for the company name, utility name for ARC, or catch phrase. This can also be left blank.
- ▶ SELECT BANNER IMAGE - These are images that have been uploaded via the **Upload new banner image** option or placed into the **banners** subdirectory in the `\arcweb\www` directory of the host system.
- ▶ UPLOAD NEW BANNER IMAGE - allows you to upload images of up to 640x100 pixels for use as the primary banner image at the top of every page. Typical use is for company logos. In order for this option to work, the anonymous user account (typically `iusr_computername` or just `IUSR`) must have list and write permissions on this `\arcweb\www\banners` directory.
- ▶ FOOTER DISPLAYS LOGO - allows to show or hide the Lieberman Software Logo in the lower left corner of every page.
- ▶ FOOTER DISPLAYS VERSION - show or hide the Account Reset Console version information in the lower right corner of every page.

Adjust Appearance Settings

Company Tagline	Account Reset Console
Select Banner Image	lieberman_horizontal.gif
Upload New Banner Image (maximum size 640x100):	Choose File No file chosen
Footer displays logo	☐
Footer displays version	☐

To configure the colors used throughout the website use the **Themes and Colors** section. The default themes are Blue, Green, and Red. When selecting these options the **User Theme** color hex codes will not change. The User Theme color hex codes will become active when the **User** theme is selected. With this option, the admin can configure any and all color settings in the product.

Themes and Colors

Themes

☒ Blue ☐ Green ☐ Red ☐ User

User Theme

Company Tagline Color	4297D7
Menu Bar Color	5C9CCC
Menu Text Color	FFFFFF
Active Menu Bar Color	2573B0
Page Header Color	DFEFFC
Page Header Text Color	363636
Page Border Color	A6C9E2
Inactive Content Color	1D5987
Active Content Color	0A1721
Alternative Table Row Color	F0F0F0

Save

Restore

Once changes have been made, be sure to click the **Save** button at the bottom of the page. To revert Account Reset Console back to its default appearance settings, click the **Restore** button at the bottom of the page, then click the **Save** button.

HOW TO USE ACCOUNT RESET CONSOLE

The following pages describe the basic use of Account Reset Console including resetting user passwords, and one's own password, how to view these actions in the programs logs, and how to run reports on users.

IN THIS CHAPTER

Accounts	48
Scheduling/Reporting	61



ACCOUNTS

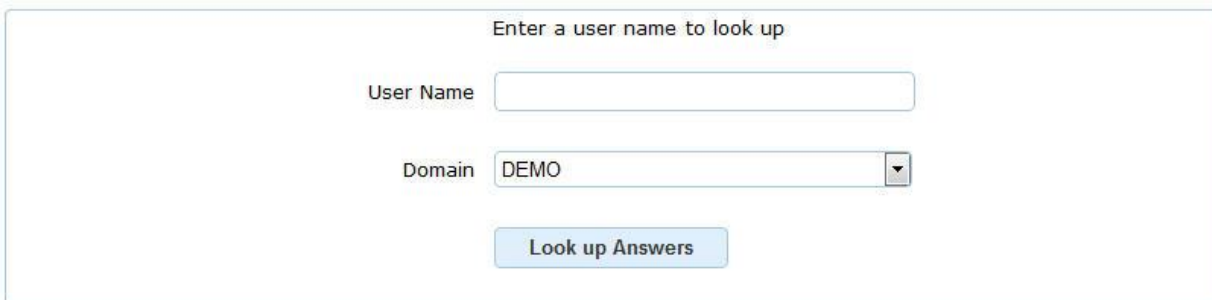
The **Accounts** area is used both by regular users and help desk. Depending on the various options and delegations configured with Account Reset Console, the Accounts menu may display different options. For example, if a user can reset other user passwords and ARC has been configured to allow resetting of one's own password both normally and via ID verification, a user will see three links on the on the Accounts menu: 1) Lookup/Reset, 2) Change My Password, 3) Setup My Identity. These options are configured in the **Help desk Reset Features** and **Self Reset Features** sections of the **Management** area.

Accounts	Scheduling/Reporting	Management	Configuration
• Lookup / Reset • Change My Password • Set Up My Identity			

LOOKUP/RESET

To begin a password reset for another user, go to **Accounts | Lookup/Reset**.

Lookup/Reset is the default page following a user login. Here they will type in the user account name to be managed, choose the correct domain, and then click **Look Up Answers**.



Enter a user name to look up

User Name

Domain

Based on whether or not user verification is turned on and the help desk user has been granted the rights to lookup this user's verification answers, the following screen will be displayed wherein a user's verification answers can be validated. If the user has not enrolled yet or enrollment is not required, ARC will go straight to the password reset screen.

If the target account has enrolled with the verification questions, the help desk user must validate N user verification questions, where N is equal to the setting defined in the **Help desk Reset Features** section of the **Management** area. The help desk user will select the check box next to the question they wish to ask, ask the user for the answer, and type in the answer into the question's answer field.

Based on the options defined in the **Help desk Reset Features** section of the **Management** area, the help desk user may see the answer text or it may be obfuscated as shown in the image below.

Once the answer is input, the help desk user will click the **Verify** button. If the answer is incorrect, there will be a notification as such, otherwise, the help desk user will be brought to the final screen.

Enter identity information for DEMO\susan

Select any 1 question(s) to verify the user's identity

Question	Answer	Status
What is your first pet's name?		
What is your mother's maiden name?		

Verify

Ensure the first option to **Reset the user account password** is selected, type in the new password twice, and examine the three options below the password input fields. These options are defined in the **Help Desk Reset Features** section of the **Management** area as to whether they will be mandatory, optional (default), or disabled. If they are left as optional, they will all be enabled.

Once the help desk user has set the password and configured the options, click the **Reset Account** button to reset the password.

Enter a new password (twice) and select options for the account to be reset.

User Name

susan

Domain

DEMO

☒ Reset the account password

New Password

Password (again)

☒ Enable account if disabled

☒ Unlock account if locked

☒ Require that reset passwords be changed on next login

Reset Account

If the reset is successful, logging messages above the user name to that effect will be displayed. Similarly, if there are failures. The operation that failed will also indicate that there was a failure.

Results

```
3/20/2012 1:39:48 PM DateOfExpiration by [DEMO\fred] for account [DEMO\susan] : Success. Server: \\2K8R2-DC
3/20/2012 1:39:48 PM Password by [DEMO\fred] for account [DEMO\susan] : Success. Server: \\2K8R2-DC
3/20/2012 1:39:48 PM PwdExpired by [DEMO\fred] for account [DEMO\susan] : Failure. Server: \\2K8R2-DC
- Error: 87 (User's password never expires.)
3/20/2012 1:39:48 PM SetAccountFlags by [DEMO\fred] for account [DEMO\susan] : Setting Flag Expired to FALSE
```

All actions from the time of user login, verification, and password reset attempt will be logged. The logs are accessible at **Scheduling/Reporting | View Logs**.

CHANGE MY PASSWORD

For a user to reset their own password, go to **Accounts | Change My Password**.

Account Reset Console allows for users to reset their own password in one of two scenarios:

- ▶ If the user knows their current password
- ▶ If the user has forgotten their current password but have enrolled for self service reset

This section details how a user may reset their password using Account Reset Console if they know their current password. If a user needs to reset their forgotten password and/or unlock their locked out account, please see the next section, **Change a Forgotten Password**.

This option is useful in the scenario where a user has access to a neighbor's computer, secured kiosk, or access to a published web page.

In order for a user to be able to reset their own password using account reset console when the password is known, the option to **Allow users to change their own passwords by logging into ARC** must be enabled in the **Management | Self Reset** section. For more information on this and other options please see **Self Reset Features**.

Once the afore mentioned options are enabled, a user may log into the web console, select **Change My Password** from the **Accounts** menu. Once there, they must input a new password twice, then click the **Change** button.



The screenshot shows a web form for changing a password. At the top, it says "Please enter your new Password twice to reset." Below this, there are two input fields. The first is labeled "New Password" and the second is labeled "Repeat New Password". Both fields are empty. Below the input fields is a blue button labeled "Change".

CHANGE A FORGOTTEN PASSWORD - WEB

Change a Forgotten Password is available from the ARC Web Login screen when the feature is enabled.

Account Reset Console allows for users to reset their own password in one of two scenarios:

- ▶ If they know their current password
- ▶ If they have forgotten their current password but have enrolled for self service reset

This section details how a user may reset their password using Account Reset Console if they have forgotten their password and/or locked out their account. The previous section, **Change My Password**, details how a user may reset their password using Account Reset Console if they know their current password.

This option is useful in the scenario where a user has locked out their account, has forgotten their password, or both.

Note: Additionally, there is a Logon Provider to integrate into the CTRL+ALT+DEL logon screen of Windows to allow a user to perform the same actions if they are unable to use another computer or there is no secured kiosk. This item can be downloaded from the Lieberman Software website from the same page as Account Reset Console. Instructions for installation and use of these items is included with the download.

In order for a user to be able to reset their own password using account reset console when they have forgotten their password, the option to **Allow users to reset their own passwords via ID verification (Website)** or **Allow users to reset their own passwords via ID verification (Logon Provider)** must be enabled in the **Management | Self Reset** section. For more information on this and other options please see **Self Reset Features**. Further, a user must have previously enrolled with user verification questions

using the **Setup My Identity** feature of account reset console. Account Reset Console provides for a nag feature to alert the user that they need to enroll. This can be configured on the **Account Tasks** section under **Scheduling/Reporting**.

A user may reset their own forgotten password or locked out account by opening the Account Reset Console website (or optionally by clicking the link on their CTRL+ALT+DEL dialog prior to logging in) and selecting the **Reset Password / Unlock** button at the bottom of the ARC login page.



The screenshot shows the 'Account Reset Console' login interface. At the top, there is a red logo and the text 'LIEBERMAN SOFTWARE'. Below this, the title 'Account Reset Console' is displayed in large white letters. The main section is titled 'Please log in' and contains three input fields: 'User Name', 'Password', and 'Domain'. The 'Domain' field is a dropdown menu currently showing 'DEMO'. Below these fields is a 'Log In' button. At the bottom, there is a link 'Forgot your password / Locked out?' and a button labeled 'Reset Password / Unlock'.

LIEBERMAN SOFTWARE

Account Reset Console

Please log in

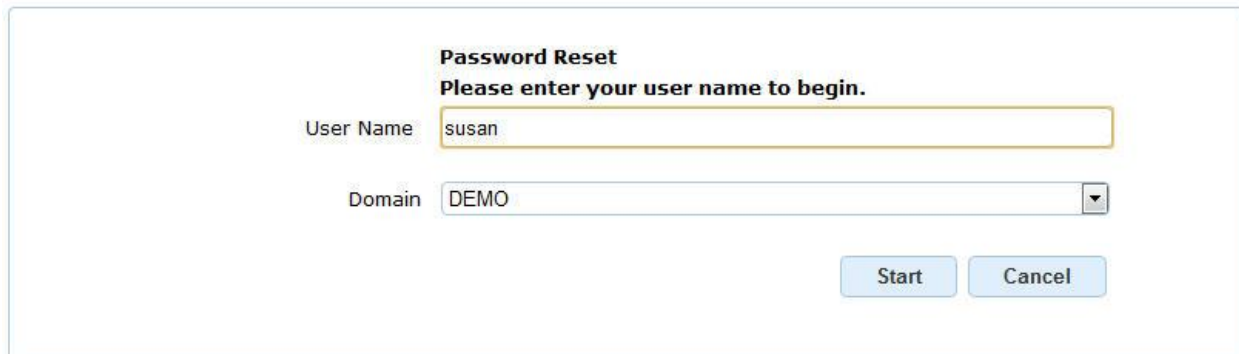
User Name

Password

Domain

[Forgot your password / Locked out?](#)

Enter the username, select the correct domain, then click **Start**.

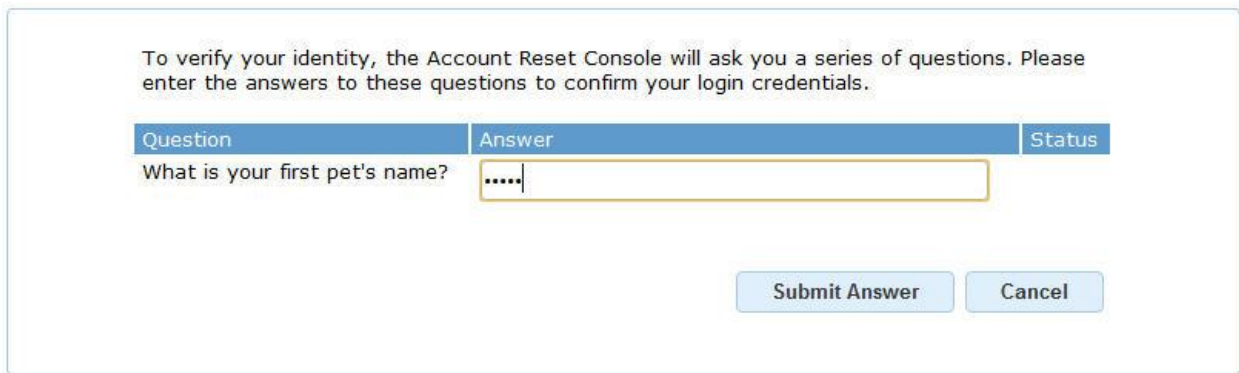


Password Reset
Please enter your user name to begin.

User Name

Domain

Answer any verification questions that are prompted. Answers are not case sensitive. Click **Submit Answer**. If the answers are correct, the process will move forward. If any of the answers are incorrect, a brief error message will appear and the answers must be corrected. If incorrect answers are input N number of times, where N is defined in **Management | Self Reset options**, the user will be locked out of the product for N minutes, and the user, help desk, and ARC administrator may be notified.



To verify your identity, the Account Reset Console will ask you a series of questions. Please enter the answers to these questions to confirm your login credentials.

Question	Answer	Status
What is your first pet's name?		

Based on the options defined in Management | Self Reset Options, the user may be able to select among up to three actions:

- ▶ Unlock the account only
- ▶ Reset the password only
- ▶ Unlock and Reset the Password

The user will enter the new password twice, then click **Change**.

Self Service Options

- ☐ Unlock the account only
- ☐ Reset the password only
- ☒ Unlock and Reset the Password

Self Service Actions

Please enter your new Password twice to reset.

User Name DEMO\susan

New Password

Repeat New Password

Once the user clicks change, logging messages will appear indicating success or failure for each step ARC goes through during a reset/unlock/notify process.

Results

3/22/2012 5:49:33 AM Password by [DEMO\susan] for account [DEMO\susan] : Success. Server: \\2K8R2-DC2

3/22/2012 5:49:33 AM PwdExpired by [DEMO\susan] for account [DEMO\susan] : Success. Server: \\2K8R2-DC2

3/22/2012 5:49:33 AM SetAccountFlags by [DEMO\susan] for account [DEMO\susan] : Setting Flag Expired to FALSE

CHANGE A FORGOTTEN PASSWORD - LOGON PROVIDER

Change a Forgotten Password is available from the Logon Provider when the feature is enabled.

Account Reset Console allows for users to reset their own password in one of two scenarios:

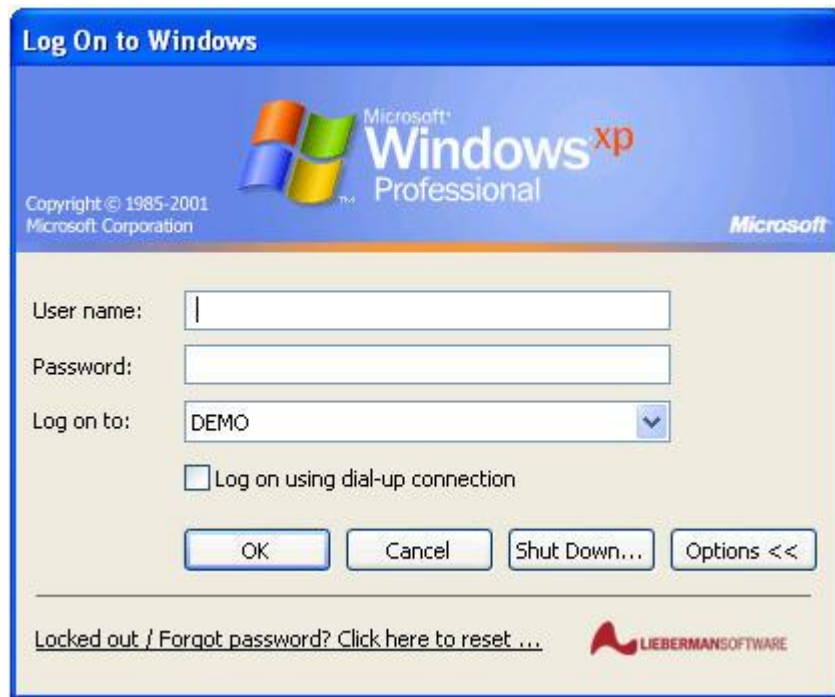
- ▶ If they know their current password
- ▶ If they have forgotten their current password but have enrolled for self service reset

This section details how a user may reset their password using Account Reset Console Logon Provider if they have forgotten their password and/or locked out their account.

This option is useful in the scenario where a user has locked out their account, has forgotten their password, or both and the user has enrolled their verification questions.

In order for a user to be able to reset their own password using account reset console when they have forgotten their password, the option to **Allow users to reset their own passwords via ID verification (Login Provider)** must be enabled in the **Management | Self Reset** section. For more information on this and other options please see **Self Reset Features**. Further, a user must have previously enrolled with user verification questions using the **Setup My Identity** feature of account reset console. Account Reset Console provides for a nag feature to alert the user that they need to enroll. This can be configured on the **Account Tasks** section under **Scheduling/Reporting**.

Once the user hits CTRL+ALT+DEL to login, a new area on the login dialog will appear below the username and password fields for the Logon Provider. Click the link to begin the self reset process.



Enter the username, select the correct domain, then click **Next**.



The screenshot shows a Windows-style application window titled "Account Reset Console - Identity". The window has a blue header bar with the title. Below the header, there is a logo on the left and the text "Password Reset Account Reset Console" in large, bold, white letters. Below this, in smaller white text, is "Copyright 2007 Lieberman Software" and "LIEBERMAN SOFTWARE". The main area of the window is light beige and contains the instruction: "Please enter/verify your user name and domain. Press Next to start." Below this instruction are two input fields. The first is labeled "User name:" and contains the text "susan". The second is labeled "Logon to:" and is a dropdown menu showing "DEMO". At the bottom of the window, there are three buttons: "Help", "Cancel", and "Next".

Account Reset Console - Identity

Password Reset
Account Reset Console

Copyright 2007 Lieberman Software LIEBERMAN SOFTWARE

Please enter/verify your user name and domain. Press Next to start.

User name:

Logon to:

Help Cancel Next

Answer any verification questions that are prompted. Answers are not case sensitive. Click Submit Answer. If the answers are correct, the process will move forward. If any of the answers are incorrect, a brief error message will appear and the the answers must be corrected. If incorrect answers are input N number of times, where N is defined in Management | Self Reset options, the user will be locked out of the product for N minutes, and the user, help desk, and ARC administrator may be notified. Click **Next** to continue.



Account Reset Console - Verification

 **Password Reset**
Account Reset Console

Copyright 2007 Lieberman Software LIEBERMAN SOFTWARE

What is your first pet's name?

.....

Help Cancel Next

Based on the options defined in Management | Self Reset Options, the user may be able to select among up to two actions: Unlock and Reset the Password or **Unlock the account only**.

If resetting the password, the user will enter the new password twice, then click **Next**.



The dialog box is titled "Account Reset Console - Reset Password". It features a blue header bar with a red logo on the left and the text "Password Reset Account Reset Console" in the center. Below the header, it says "Copyright 2007 Lieberman Software" on the left and "LIEBERMAN SOFTWARE" on the right. The main area has a light beige background. It contains two text input fields: "New Password:" and "Retype New Password:", both filled with black dots. Below these is a checkbox labeled "Unlock the account only". A "Password Requirement:" section lists: "The password must contain at least one of the following three types", "Upper case", "Lower case", "Number", and "Special character". Below this is a "Contact:" field with the email "sales@liebsoft.com". At the bottom are three buttons: "Help", "Cancel", and "Next".

Any success or failure messages will appear on a subsequent dialog. If the reset/unlock was successful, the user may logon as normal.



SETUP MY IDENTITY

To enroll your identity for self service reset/unlock, go to **Accounts | Setup My Identity**.

This page is used to configure verification answers for self service password reset / account unlock. The questions presented on this page are defined by the administrator of Account Reset Console. For more information on configuring questions, see the **Verification** section in the **Configuration** area.

A user must supply answers to all questions posed. When the verification questions are not complete, there will be a notice that states, **Your verification information is not complete**. Once all of the questions are answered, the user will click the **Save** button.

Answers provided on this page are not case sensitive, though constraints defined in the **Self Reset Features** section will determine what kind of answers are allowed.

You are required to complete 2 out of the following 3 question(s).

Question	Answer	Status
What is your first pet's name?		
What is your mother's maiden name?		
What is your favorite color?		

Save

Your verification information is not complete.
You must complete all required questions before the verification system will function.

If there are no problems with the answers supplied for the questions, the page will display a notice, **Your verification information is complete** and the answers will have green check marks to the right of them.

You are required to complete 2 out of the following 3 question(s).

Question	Answer	Status
What is your first pet's name?	kitty	✓
What is your mother's maiden name?	smith	✓
What is your favorite color?	red	✓

Save

Your verification information is complete.



SCHEDULING/REPORTING

The **Scheduling/Reporting** area of Account Reset Console is used to view the logs that are kept for all password reset functions in Account Reset Console as well as create various notification and management reports.

VIEW LOGS

To view activity logs, go to **Scheduling/Reporting | View Logs**.

Account Reset Console keeps track of all successful and failed logon attempts as well as all password reset actions and notifications. These are stored in the default logging database and can be accessed within ARC from the **View Logs** section under **Scheduling/Reporting**.

In order to view the logs, a group must have been granted access to **View console Logs and Task Reports** from **Management | Program Access**.

To see who has successfully or unsuccessfully attempted logging into the Account Reset Console website, choose **Access Log**. To see the actions performed by various users against themselves or other users, select the 'Action Log' radio button. Choose a date range (presented as MM/DD/YYYY), and optionally choose a user to filter for, then click the **Display Log** button. Clicking in the Date/Time field will also display a date picker. You may additionally filter times with a 24 hour time filter such as 12/09/2008 14:30:30.

Display Activity Log

Event Type ☒ Access ☐ Action

From To

User Name

The logs will show the date the action occurred, the IP address it occurred from, the action, the user who performed the action, the account it was performed against, and the status of the action.

Logs may be exported by choosing the output type as CSV or XML and the clicking the **Save** button. The user will be prompted for the directory in their machine to save the log to.

Page 1 of 2			Select a page: 1 ▼
Date	IP Address	Action	User
3/21/2012 3:39:19 PM	127.0.0.1	logon success	DEMO\LSCADMIN
3/21/2012 6:41:29 PM	192.168.8.4	logon success	DEMO\LSCADMIN
3/21/2012 6:48:42 PM	192.168.8.4	logon success	DEMO\LSCADMIN
3/21/2012 6:55:08 PM	192.168.8.4	logon success	DEMO\LSCADMIN
3/22/2012 5:43:57 AM	192.168.20.183	multifactor logon success	DEMO\SUSAN
3/22/2012 5:56:56 AM	192.168.20.183	logoff	DEMO\SUSAN
3/22/2012 8:34:24 AM	192.168.20.183	logon success	DEMO\SUSAN
3/22/2012 8:35:13 AM	192.168.20.183	logoff	DEMO\SUSAN
3/22/2012 8:35:34 AM	192.168.20.183	logon success	DEMO\SUSAN
3/22/2012 8:35:46 AM	192.168.20.183	logoff	DEMO\SUSAN
Record 1-10 of 13			Items Per Page 10 ▼

Save Output

☒ CSV ☐ XML

Save

ACCOUNT TASKS

To create account tasks, go to **Scheduling/Reporting | Account Tasks**.

Account Tasks reports are used to provide the administrator reports of users whose passwords will expire, users who have become inactive (have not logged on in a while), and users who have not enrolled for self service reset. Account Tasks reports can also notify the specific user and take action against the user account such as disabling accounts.

By default there are no account task/reports configured. Create a task by choosing the task type, providing a name, and configuring the various options asked for within the task properties. The steps outlined below identify how to create a management report; the steps are the same no matter what report type.

First type in a report name, choose a report type, and click the **Add** button.

- ▶ Password Expiration - find users whose passwords will expire in N number of days. A value of 0 days will look for account's whose passwords are currently expired.
- ▶ Self Reset Configuration - find users whose password verification information is not completely filled out.
- ▶ Account Inactivity - find users whose accounts have not logged on in N days.

Configure Scheduled Tasks Here

Active Tasks

Name	Type	Action
------	------	--------

Inactive Tasks

Name	Type	Action
------	------	--------

[Run Selected Tasks Now](#)**Add New Task**

Task Name:

Task Type:

- ☒ Password Expiration
☐ Self Reset Configuration
☐ Account Inactivity

[Add](#)

When a task is first added, it will show under the 'Inactive Reports' heading. The task must be edited before it is useful; identify the report parameters. Once those are done, activate the question or leave it inactive. Leaving a question inactive simply means it will not run on an automatic scheduled basis. Tasks may be run ad-hoc at any time by selecting the report and clicking the 'Run Selected Reports Now' button.

Configure Scheduled Tasks Here

Active Tasks

Name	Type	Action

Inactive Tasks

Name	Type	Action
☐ Password Expiry	Password Expiration	Activate Edit Delete

Add New Task

Task Name:

Task Type:

- ☒ Password Expiration
- ☐ Self Reset Configuration
- ☐ Account Inactivity

To run the report to run on a scheduled basis (Active Task), choose the days for the report to run and whether the task should run at noon or at midnight. The task will run as a result of one of two scheduled tasks (probably called AT1 and AT2) in the scheduled tasks folder visible in control panel.

Identify the target global group that Account Reset Console will report on. Once the name is typed, click the **Add** button and the group name will appear in the Target Groups list. If there are users who are members of any of the groups being reported on who should not be included as part of the report, such as service or process accounts, type in their names in the format of domainName\userName in the **Filter Users** list. Multiple entries are separated by a semi-colon ';'.

Depending on the report type, a number may also be required, such as **Find accounts whose password will expire in N days**. N is the inclusive number of days from today. For example, if you input a value of 60, the report will find any users whose passwords will expire any time within the next 60 days.

Account Tasks provide additional functionality such as the ability to disable or enable an account that meets the criteria of the report or to notify that user that they were found by the report. If 'Send the user an email' is selected, ARC will lookup the user's email address attribute in Active Directory for this information.

Optionally provide an email address to email the report results to. If this value is not provided, the reports can still be viewed by examining the **View Task Results** section and choosing the report from the list.

Once options are configured, click either **Save** or **Save and Run Now** which would initiate the report right now. To exit without making any changes, click **Return**.

Schedule

☒ Sunday

☒ Monday

☒ Tuesday

Runs on: ☒ Wednesday

☒ Thursday

☒ Friday

☒ Saturday

At: ☐ Noon ☒ Midnight

Last Run: Never

Target

Target Groups:

DEMO

Domain Users

Add

Filter Users:

Ignore user names which contain the following substrings (separate by ;)

Actions

Details: Find accounts whose password will expire in

14

 day(s)

☐ Disable the user's account

☐ Enable the user's account

☒ Send the user an email

To #RealName\$:

your account will expire in #PwdDaysToExp#. Please change your password before it expires to avoid having your account disabled.

☒ PlainText ☐ HTML

User email keywords:
#RealName# - User's full name as stored in Active Directory.
#PwdDaysToExp# - Days until the user's password expires

Email Result To:

Save

Save and Run Now

Return

Don't forget, leaving a task in the inactive reports area will cause the report to never run despite any scheduling option configured within the task. To allow a task to run on a scheduled basis, provide the days for it to run and activate the question by clicking the **Activate** link next to the question.

VIEW TASK RESULTS

View Tasks Results is located in the Scheduling/Reporting area.

Any task which has been run can have its results in the **View Reports** section of the **Scheduling/Reporting** area.

There are two lists to choose the report from. The **Most Recent Tasks** list contains the 10 most recent reports. The **Tasks By Name** list lists all reports by name that have been run. By clicking on links in that list, a list all the run times for a particular report will be displayed and those reports can be viewed.

Most Recent Tasks:

Name	Date	Status
Password Expiry	3/22/2012 8:59:38 AM	Some actions could not be completed.
Password Expiry	3/22/2012 8:59:02 AM	This task was run on no groups.
Password Expiry	3/22/2012 8:58:49 AM	This task was run on no groups.

Tasks By Name:

Name	Last Run Date
Password Expiry	3/22/2012 8:59:38 AM

Below is a sample report. The report will only contain entries that match the task criteria. If searching for users whose passwords will expire in N days, the report will only contain users matching that criteria. The task report will also contain information about any subsequent task it was supposed to perform such as email users.

Configuration

- Task Description: Find accounts that expire in 1000 days.
- Target Groups: DEMO\domain users.
- Task Action(s): email the user.

Page 1 of 2		Select a page: 1 ▼	
Domain	User	Action	Results
DEMO	Joe	Match criteria	OK
DEMO	Joe	Send alert email	Failure: no email address available
DEMO	dtest	Match criteria	OK
DEMO	dtest	Send alert email	Failure: no email address available
DEMO	jeff	Match criteria	OK
DEMO	jeff	Send alert email	OK
DEMO	krbtgt	Match criteria	OK
DEMO	krbtgt	Send alert email	Failure: no email address available
DEMO	user01	Match criteria	OK
DEMO	user01	Send alert email	Failure: no email address available
Record 1-10 of 12		Items Per Page 10 ▼	

MANAGE SYNCHRONIZATION

To view ARC synchronization tasks, go to **Scheduling/Reporting | Manage Synchronization Settings**.

Synchronization is used to save all of ARCs settings to its main database. The purpose of this is two fold:

- ▶ If there is need for a restoration of Account Reset Console to a new server
- ▶ Multiple ARC Web Servers are configured in an NLB scenario

In the latter scenario, changes made to one ARC server's configuration would be replicated to the other ARC servers.

Configure Scheduled Synchronization Here
Active Synchronization

Name	Type	Action
☐ SaveToDB	Save Settings to Database	Deactivate Edit Delete

Inactive Synchronization

Name	Type	Action
------	------	--------

Run Selected Synchronization Now

Add New Synchronization Schedule

Name:

Type:

- ☒ Save Settings to Database
- ☐ Load Settings from Database

Add

To write the settings to the database, supply a name for the **Synchronization Schedule** then click **Add**. This will add the update task in a deactivated state. Such a job could be run at will be selecting the job and clicking **Run Selected Synchronization Now**.

To read settings from the database, supply a name for the **Synchronization Schedule** and choose the option to **Load Settings from Database**, then click **Add**. This will add the update task in a deactivated state. Such a job could be run at will be selecting the job and clicking **Run Selected Synchronization Now**.

To allow the jobs to run on a automatically on a schedule, the jobs must be activated and edited to include a schedule. To edit a job, click the **Edit** link next to the job.

Schedule

☐ Sunday

☐ Monday

☐ Tuesday

Runs on: ☒ Wednesday

☐ Thursday

☐ Friday

☒ Saturday

At: ☐ Noon ☒ Midnight

Last Run: Never

ActionsEmail Result To:

Save

Save and Run Now

Return

Choose the day(s) for the synchronization to run and at what point (noon or midnight) the synchronization should occur. If details of the synchronization should be emailed, supply the email address for the notification in the **Email results to** field.

Choose to **Save** when all desired changes have been made.

VIEW SYNC RESULTS

To view ARC synchronization task results, go to **Scheduling/Reporting | View Synchronization Results**.

View Sync Results provides logging information for all synchronizations that have occurred.

There are two lists to choose the report from. The **Most Recent Synchronization** list contains the 10 most recent reports. The **Synchronization By Name** list lists all reports by name that have been run. By clicking on links in that list, a list all the run times for a particular report will be displayed and those reports can be viewed.

Most Recent SyncTasks:

Name	Date	Status
SaveToDB	3/22/2012 9:09:13 AM	All actions were completed successfully.

SyncTasks By Name:

Name	Last Run Date
SaveToDB	3/22/2012 9:09:13 AM

Below is a sample report.

SyncTasks: SaveToDB

Run on: 3/22/2012 9:09:13 AM
All actions were completed successfully.

Configuration

Task Description: Save settings to database
Task Computer Name: 2K332-UMPWEB
Task Action(s): email the user.

Domain	User	Action	Results
DEMO	lscadmin	SyncToDB	OK

INDEX

A

ACCOUNT TASKS • 58, 62

ACCOUNT TASKS • 70

ACCOUNTS • 54

ADDING OR UPDATING VERIFICATION
QUESTIONS • 26

ADDING OR UPDATING VERIFICATION
QUESTIONS • 28

APPEARANCE • 49

C

CHANGE A FORGOTTEN PASSWORD -
LOGON PROVIDER • 62

CHANGE A FORGOTTEN PASSWORD -
WEB • 57

CHANGE A FORGOTTEN PASSWORD -
WEB • 57

CHANGE MY PASSWORD • 57

CHANGE MY PASSWORD • 56

CONFIGURATION • 20

CONFIGURE EMAIL SETTINGS • 27, 42, 47

CONFIGURE EMAIL SETTINGS • 48

D

DATA SOURCES • 21

DOMAIN DETAILS • 33

DOMAIN DETAILS • 34

DOMAINS • 20

DOMAINS • 33

G

GROUP ACCESS • 37

GROUP ACCESS • 38

H

HELP DESK RESET FEATURES • 54, 55

HELP DESK RESET FEATURES • 39

HOW TO USE ACCOUNT RESET CONSOLE
• 53

I

INITIAL CONFIGURATIONS • 13

INPUT THE LICENSE • 17

L

LICENSE AGREEMENT • 7

LIMITED WARRANTY • 8

LOG CONFIG • 23

LOOKUP/RESET • 54

M

MANAGE SYNCHRONIZATION • 77

MANAGEMENT • 20, 27, 42, 47, 54, 55

MANAGEMENT • 37

P

PRE-USAGE CONSIDERATIONS • 11

PROGRAM ACCESS • 37

S

SCHEDULING/REPORTING • 69

SECURITY • 34

SELF RESET FEATURES • 38, 39, 54, 57, 58, 62,
67

SELF RESET FEATURES • 43

SETUP MY IDENTITY • 58, 62

SETUP MY IDENTITY • 66

SUPER USERS • 35

T

THE FIRST LOGIN SCREEN • 14

V

VERIFICATION • 67

VERIFICATION • 25

VIEW LOGS • 69

VIEW SYNC RESULTS • 79

VIEW TASK RESULTS • 76